AMENDMENTS

Claim amendments:

The following shows the status of all claims:

Claim 1. (Currently Amended) A computer system ~~for preventing~~ configured to prevent illegal ~~use of software~~access to secret information, comprising:

secret information storage means for storing secret information to be protected from illegal access;

cryptosystem key storage means for storing a cryptosystem key used for decrypting ~~the secret~~ encrypted secret information stored in the secret information storage means;

illegal access determining means for determining whether an ~~illegal~~ access to the system ~~is performed~~ is illegal; and

cryptosystem key updating means for updating the cryptosystem key used for decrypting encrypted secret information stored in the secret information storage means upon each access to the system,~~:~~

wherein, if an access to the system is legal, the cryptosystem key updating means updates the cryptosystem key for decrypting encrypted secret information prior to decrypting the secret information, such that the cryptosystem key will correctly decrypt the secret information, and~~providing the same key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if the illegal access determining means detects no illegal access;~~

wherein, if an access to the system is illegal, the cryptosystem key updating means updates the cryptosystem key for decrypting encrypted secret information prior to decrypting the secret information, such that the cryptosystem key will not correctly decrypt the secret information.~~providing different keys for the above two kinds of cryptosystem keys if the illegal access determining means detects an illegal access; and~~

~~wherein the cryptosystem key updating means updates the above two kinds of cryptosystem keys for each access to the system.~~

Claim 2. (Currently Amended) A method for preventing illegal ~~use of software~~access to secret information, the method used in a system which comprises a secret information storage means for storing encrypted secret information to be protected from illegal access and a cryptosystem key storage means for storing a cryptosystem key used for decrypting ~~the~~ encrypted secret information stored in the secret information storage means, the method comprising the steps of:

determining whether an ~~illegal~~ access to the system is ~~performed~~illegal;

and for each access to the system,

if the access to the system is legal, updating the cryptosystem key for decrypting encrypted secret information prior to decrypting the secret information, such that the cryptosystem key will correctly decrypt the secret information, and~~providing the same updated key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if no illegal access is detected in the step of determining whether an illegal access to the system is performed;~~

if the access to the system is illegal, updating the cryptosystem key for decrypting encrypted secret information prior to decrypting the secret information, such that the cryptosystem key will not correctly decrypt the secret information.~~providing different updated keys for the above two kinds of cryptosystem keys if an illegal access is detected in the step of determining whether an illegal access to the system is performed.~~

Claim 3. (Currently Amended) A storage medium storing a computer-executable program for preventing illegal ~~use of software~~access to secret information, the program used in a system which comprises a secret information storage means for storing encrypted secret information to be protected from illegal access and a cryptosystem key storage means for storing a cryptosystem decrypting ~~the~~ encrypted secret information stored in the secret information storage means, the program including the processes of:

determining whether an ~~illegal~~ access to the system is ~~performed~~illegal; and

for each access to the system,

if the access to the system is legal, updating the cryptosystem key for decrypting encrypted secret information prior to providing the secret information, such that the cryptosystem key will correctly decrypt the secret information, and~~providing the same updated key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if no illegal access is detected in the step of determining whether an illegal access to the system is performed;~~

if the access to the system is illegal, updating the cryptosystem key for decrypting encrypted secret information prior to providing the secret information, such that the cryptosystem key will not correctly decrypt the secret information.~~providing different updated keys for the above two kinds of cryptosystem keys if an illegal access is detected in the step of determining whether an illegal access to the system is performed.~~

Claim 4. (Original) A system for preventing illegal use of software as claimed in claim 1, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

Claim 5. (Original) A method for preventing illegal use of software as claimed in claim 2, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

Claim 6. (Original) A storage medium storing a computer-executable program for preventing illegal use of software as claimed in claim 3, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

Claim 7. (Original) A system for preventing illegal use of software as claimed in claim 1, wherein the system is applied to an IC card.

Claim 8. (Original) A method for preventing illegal use of software as claimed in claim 2, wherein the system in which the method is used is applied to an IC card.

Claim 9. (Original) A storage medium storing a computer-executable program for preventing illegal use of software as claimed in claim 3, wherein the system in which the program is used is applied to an IC card.

Claim 10. (New) A computer system as claimed in claim 1, wherein, upon each access to the system, the secret information is correctly decrypted with a cryptosystem key stored in the cryptosystem key storage means, the secret information is then re-encrypted using a different cryptosystem key, and the cryptosystem key for decrypting the secret information is then updated in accordance with whether the attempted access is legal or illegal.

Claim 11. (New) The computer system as claimed in claim 10, wherein the access to the computer system is an attempted access to the secret information.

Claim 12. (New) A method as claimed in claim 1, wherein, upon each access to the system, the secret information is correctly decrypted with a cryptosystem key stored in the cryptosystem key storage means, the secret information is then re-encrypted using a different cryptosystem key, and the cryptosystem key for decrypting the secret information is then updated in accordance with whether the attempted access is legal or illegal.

Claim 13. (New) The method as claimed in claim 12, wherein the access to the computer system is an attempted access to the secret information.

Claim 14. (New) A storage medium as claimed in claim 1, wherein, upon each access to the system, the secret information is correctly decrypted with a cryptosystem key stored in the cryptosystem key storage means, the secret information is then re-encrypted using a different cryptosystem key, and the cryptosystem key for decrypting the secret information is then updated in accordance with whether the attempted access is legal or illegal.

Claim 15. (New) The storage medium as claimed in claim 14, wherein the access to the computer system is an attempted access to the secret information.